情報セキュリティと個人情報の保護

亀田彰喜　勝木太一

概　要

情報通信技術の発達により、またそれに伴う情報ネットワークの発達により、多くの情報を大量に取扱うことが可能になって、情報の取扱いが重視されるようになってきた。さらに、情報のデジタル化により、また情報技術と通信技術の統合によって情報ネットワークは飛躍的に進歩してきた。特に、情報は商品価値を持つがその価値は情報のコンテンツによって決まる。

今日のように、インターネットなどによって情報がネットワークを通して、情報が地球規模で送られるようになってきたのに伴い、個人情報の不正な侵害も国際化してきている。そのため、欧米諸国において1960年頃から個人情報保護に関心がもたれ、法制化が各国で検討された。

我が国において、個人情報の保護に対して関心がもたれ、実際に、政府が検討を始めたのは昭和40年末であった。そして、行政機関におけるコンピュータの導入に伴って、処理される個人の情報の取扱いについての検討がなされた。昭和60年代より、個人情報保護に関しては検討されてきていたが、平成15年５月23日に個人情報保護法が成立し、その後、５月30日に一部施行され、平成17年４月１日より完全施行されることとなった。

情報ネットワークにより、世界中のコンピュータが接続されることから、地理的、時間的超越のもとに随時に必要な情報を入手することが可能になった。それと同時に、今日のネットワーク社会に対して、多くの危険と障害が発生してきている。しかし、今後ともこの情報ネットワークの利便性を享受し、我々の生活の安全と社会の発展を進展させるためには、セキュリティポリシーに基づいた情報のセキュリティ対策が重要である。

個人情報の保護に関する法律が施行されて以来、個人情報に対して過剰に反応するようになったようである。今後、個人情報に対する意識過剰は社会活動や経済活動にも影響をもたらしかねないかもしれない。このことが個人情報保護に対する今後の検討課題である。

１．はじめに

インターネットはビジネスや日常生活に飛躍的に利便性をもたらした。しかし、反面、近年、個人情報の流出やホームページの改ざん、およびウィルスやワームなどによるネット犯罪も増加してきた。このようなネット犯罪を防止するためには、インターネットおよび情報通信を利用する者が情報セキュリティに対する認識と意識を待たせなければならない。そして、組織内でセキュリティ対策を講じると共に、セキュリティ対策のための人材育成が必要である。セキュリティ対策が不備である場合は、ホームページの改ざんやウィルス等により業務に支障をきたすとともに、個人情報の漏洩などは信用の失墜につながる。

このように現代の地球規模の情報ネットワーク網は、情報技術の発展によって我々の生活の利便性を高めてくれた。と同時に、多種多様な情報の入手を可能にした。すなわち、大量の個人情報の収集を容易にしている。大量に収集された個人情報は、本人の知らないうちにデータベース化され、蓄積され、本人の同意もないまま、これらの個人情報が利用されている。そのことは多くの社会的なトラブルを噴出させることになった。しかし、個人情報の取扱いがいかに慎重であっても、個人情報の管理者や担当者自身が、個人情報の漏洩にかかわった場合は防止が困難である。そのため、行政機関や企業内における個人情報保護に対する漏洩防止の教育体制が必要である。個人情報の漏洩は、その行政機関や企業が社会的信用を失うだけでなく、場合によっては損害賠償を求められることがある。

一般企業だけでなく、国や地方公共団体においても個人情報の取扱いには慎重にならねばならない。最近では特に、個人情報を不正に使用し、詐欺などに使用するなどし、社会問題を引き起こす事件が急増するようになってきた。そのため平成17年４月１日に個人情報の保護に関する法律が施行され、個人情報の取扱いを法制化し、その法の下に個人情報の漏洩および悪用をいかに防止するかが重要な問題となった。

そこで、各国の個人情報保護の取組みと施策および情報セキュリティ対策について述べる。

２．情報セキュリティと各国の個人情報の取扱いと問題点

情報ネットワークの世界的な発展に伴って多くのリスクやネット障害が発生し、社会的な問題になってきている。不正アクセスによるホームページの改ざんやシステムの破壊による障害事件などである。さらに、個人情報の流出なども発生し、行政機関や企業における信用にも影響を与えるようになってきている。また、各関係省庁からは「セキュリティ対策のガイドライン」が作成されて、セキュリティに対する取り組みを促している。そして、現在ではセキュリティ対策は組織の自己責任として、セキュリティポリシーを策定しセキュリティ対策を実施する必要がある。

情報技術の進歩と発展に伴って、単体で扱われていた情報処理がホストコンピュータと端末との接続やパソコン同士の接続、ワークステーション等の接続によってネットワークが構成されるようになっていった。そして、単体で処理されていた情報が広くネットワークのもとで処理されるようになった。当初は利便性と効率性のもとにネットワークは、技術開発が急速に進んだことも相俟って、世界的に広がっていった。ところが最近情報の技術の普及に比例して、情報の技術を悪意に使用する者が多くなり、ネットワーク社会を混乱させてきている。そのため、ネットワークに対するセキュリティ技術が求められるようになるとともに、ネットワーク上の情報を悪意をもって利用される事態を防止する手段が

求められるようになってきた。特に最近、個人の情報を不正に取得し、悪意に使用される事態が急増するようになった[1)]。

個人情報保護は個人の人権に係わる問題でもあり、公共団体や企業にとっても莫大な損失にもつながる問題でもある。個人情報漏洩事件で、多くの被害者によって訴訟を起こされ慰謝料や損害賠償を求められた場合、個人情報漏洩の被害者の数が多ければ多い程、その請求金額も莫大なものになる。そのため、個人情報の取扱いには特に慎重にならざるを得ない。しかし、近年の通信技術の発達により、一度に大量の個人情報が流出されることがある。この個人情報を不正に使用し、詐欺や脅迫等の事件に繋がる可能性がある。そのため、この個人情報保護法は個人情報の悪用に歯止めを掛けるために施行されたのである。

他に個人情報の取扱いに関する法律としては、「高度情報通信ネットワーク社会形成基本法」、「不正アクセス行為の禁止等に関する法律」、「電気通信事業法」、「有線電気通信法」、「電波法」等もあるが、最近、個人情報保護に過敏に反応し、個人情報だからとその公表等を拒否することが多くなった[2)]。

インターネットなどのように情報が、ネットワークを通して、情報が地球規模で送られるようになってきたのに伴い、個人情報の不正な侵害も国際化してきている。そのため、欧米諸国において1960年頃から個人情報保護に関心がもたれ、法制化が各国で検討された。まず最初に、世界で初めて1973年にスエーデンがデータ法を制定し、続いて1974年に米国が、さらに1977年にドイツが、そして1978年にフランスが個人情報保護の法整備を行っていった[3)]。

このように、欧米諸国では順次、個人情報保護法を整備していった。そして、OECD（経済協力開発機構）は1980年９月に「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」を採択した。これは条約のように拘束力は持たないが、プライバシーと個人の自由に係る原則（OECD８原則）を作り上げる基本になった。そして、このOECD８原則が世界各国における個人情報の法整備の基礎になった。我が国においても、平成12年１月に高度情報通信社会推進本部内に個人情報保護法制化専門委員会が発足され、幾多の審議を経た後、平成15年12月10日に「個人情報の保護に関する法律」が公布され、平成17年４月１日に施行された。

そこで、「個人情報の保護に関する法律」の法の基本となったOECD８原則を取り上げてみる。

OECD８原則[4)]

①　収集制限の原則

適法かつ公正な手段で個人情報の収集を行うこと。また、収集に当たっては本人にその旨を通知するとともに、収集への同意を得た上で収集する。

② データ内容の原則

個人データの内容は、利用目的に沿ったものであり、利用目的に必要な範囲内の内容であって、その内容が正確、完全であり最新の状態に維持する。

③ 目的明確化の原則

個人情報の収集に当たり、事前に個人情報をどのような目的で取り扱うのかを明確化しなけれならない。収集した個人情報の利用に当たっては、収集目的に合った利用のみに限定される。また、利用目的が変更された場合も同様にされる。

④ 利用制限の原則

個人データは、本人の同意がある場合と法律の規定による場合以外は利用目的に合った利用のみに限定される。

⑤ 安全保護の原則

個人情報の紛失、不正アクセス、破壊、使用、修正、開示などのリスクに対して、合理的な安全保護措置によって保護されなければならない。

⑥ 公開の原則

データ収集の実施方針等を公開して、個人データの存在や主要な利用目的や連絡先などを明示すべきこととされている。

⑦ 個人参加の原則

個人は自己に関するデータを保有しているかどうかと、その内容の確認をすることができる。また、その内容に関して異議申立てをすることができ、異議が認められた場合はそのデータの消去、修正などを求めることができる。

⑧ 責任の原則

データ管理者は、上記の諸原則を実施するための措置に従う責任を有する。

このように、OECD 8 原則においては、まず第一に個人情報の収集の制限について公正な手段で個人情報を収集し、収集に際しても本人の同意を得ることを原則としている。また、データの内容については、利用目的は必要範囲内とし、データそのものは常に正確で最新の状態にしておくこととしている。また、個人情報の取扱いにあたっては、その目的を明確にし、さらに法律の利用制限のもとに利用も限定している。また、個人情報に対して紛失、不正アクセス、破壊などのリスクに対して、安全な保護措置も求めている。さら

に、データ収集の実施方針を公開し、個人のデータの保有や内容に関して異議申立てがあった場合、データの消去や修正などの処置が求められる。そして、データ管理においての責任についても取り上げている。

コンピュータ技術の進展に伴い、1960年代にヨーロッパ諸国でコンピュータによる個人情報の処理および取扱いについて検討が始まり、1970年代に個人情報保護に関する法の整備がなされた。それに伴って、OECD（経済協力開発機構）が、1980年９月に「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」を採択した。この勧告は、ヨーロッパ諸国だけでなく、その後、国際的に個人情報保護における基準となり、このOECD８原則は、我国の「個人情報の保護に関する法律」制定のための基本となっている[5)]。

３．我が国における個人情報保護の立法化

我が国において、個人情報の保護に対して関心がもたれ、実際に、政府が検討を始めたのは昭和40年末であった。そして、行政機関におけるコンピュータの導入に伴って、処理される個人の情報の取扱いについての検討がなされた。当時の行政管理庁（現総務庁に改編）長官により諮問を受けた行政管理委員会が、個人情報に関しては行政上の適切な措置を行わなければならないと指摘した「行政機関における電子計算機利用に伴うプライバシー保護に関する制度の在り方についての中間報告」を受けて、政府は昭和51年１月に電子計算機処理において、各省庁にデータの漏洩、毀損、滅失等を防止するために「電子計算機処理データ保護管理準則」を作成した。

その後、我が国においても昭和55年９月にOECD理事会の勧告が採択された後、行政において、また、民間においても個人情報に対する対応が求められることとなった。以下、時間を追って見てみる。

我が国においても、上記のOECD理事会の勧告を受けて、昭和63年（1988年）行政機関に対して、「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」が制定された。これは社会のIT化に伴い、政府においても電子政府を、また地方行政においても電子自治体を目指すためには行政サービスの面において、個人情報の取扱いにおいて規律を設ける必要があったからである。

平成11年７月に高度情報通信社会推進本部内に個人情報保護検討部会が発足し、同年11月に高度情報通信社会推進本部内に個人情報保護検討部会から「我が国における個人情報保護システムの在り方について」の中間報告が提出され、平成12年１月に高度情報通信社会推進本部内に個人情報保護法制化専門委員会が発足する。同年10月に高度情報通信社会推進本部内の個人情報保護法制化専門委員会が「個人情報保護基本法制に関する大綱」を

出す。平成13年３月27日の第151回国会に「個人情報に関する法律案」が提出された。これを受けて、平成13年４月に総務省に行政機関等個人情報法制研究会が発足し、平成13年10月に「行政機関等の保有する個人情報の保護に関する法制の充実強化について－電子政府の個人情報保護－」をまとめ上げた。平成14年３月15日の第154回国会に「行政機関の保有する個人情報の保護に関する法律」と「独立行政法人の保有する個人情報の保護に関する法律」など４法案が提出され、平成14年４月より衆議院において個人情報の関係５法案が一括審議されたが、審議未了のままで廃案となった。

しかし、平成15年３月７日に個人情報保護の「与党三党修正要綱」を織り込んだ個人情報保護の５法案を第156回の国会に再提出され、平成15年４月８日に衆議院でこの個人情報保護の５法案を審議し、平成15年４月25日の個人情報の保護に関する特別委員会で個人情報保護の５法案を可決した。その後、平成15年５月６日に衆議院本会議でも可決した。

そして、平成15年５月９日に参議院でも個人情報保護の５法案を審議入りし、平成15年５月21日に参議院の個人情報の保護に関する特別委員会で可決した。再び衆議院に送られて、平成15年５月23日に個人情報保護の５法は可決され成立した。そして、平成15年５月30日に個人情報保護の５法は公布された[6]。

昭和60年代より、個人情報保護に関しては検討されてきていたが、平成15年５月23日に個人情報保護法が成立し、その後、５月30日に一部施行され、平成17年４月１日より完全施行されることとなった。

個人情報の保護に関する法律（平成十五年五月三十日法律第五十七号）[7]

目次

個人情報の保護に関する法律の第一章総則においては、本法の目的、定義および理念について明記している。本法の目的に関しては、国及び地方公共団体の個人情報の取扱いに対する施策と責務を明確にして、個人の権利利益を保護することとしている。そして民間事業者においても同様に、個人情報の取扱いにおける遵守すべき義務について定めている。それは、近年、情報通信の急速進展によって、個人の権利利益を侵害する問題や人権侵害にまで発展する事件が多く発生してきたためである[8)]。

また本法の第二条においては、個人情報、個人情報データベース等、個人情報情報取扱事業者、個人データ、本人などの基本的な用語の意味を定義し、それらの規律の対象と範囲を明確にしている[9)]。

そして第三条では、この個人情報の保護に関する法律に基本的に通じている精神について定義しており、個人情報が個人の人格尊重の理念の下に慎重に取り扱われるべきであって、且つ適正に取り扱うべきであるとしている。

そこで、個人情報の保護に関する法律の第一章総則の目的、定義、理念に基いて、第二章においては国及び地方公共団体の責務等について定めている。

第二章　国及び地方公共団体の責務等（第四条―第六条）[10)]

（国の責務）

第四条　国は、この法律の趣旨にのっとり、個人情報の適正な取扱いを確保するために必要な施策を総合的に策定し、及びこれを実施する責務を有する。

（地方公共団体の責務）

第五条　地方公共団体は、この法律の趣旨にのっとり、その地方公共団体の区域の特性に応じて、個人情報の適正な取扱いを確保するために必要な施策を総合的に策定し、及びこれを実施する責務を有する。

（法制上の措置等）

第六条　政府は、国の行政機関について、その保有する個人情報の性質、当該個人情報を保有する目的等を勘案し、その保有する個人情報の適正な取扱いが確保されるよう法制上の措置その他必要な措置を講ずるものとする。

2　政府は、独立行政法人等について、その性格及び業務内容に応じ、その保有する個人情報の適正な取扱いが確保されるよう法制上の措置その他必要な措置を講ずるものとする。

3　政府は、前二項に定めるもののほか、個人情報の性質及び利用方法にかんがみ、個人の権利利益の一層の保護を図るため特にその適正な取扱いの厳格な実施を確保する必要がある個人情報について、保護のための格別の措置が講じられる必要な法制上の措置その他の措置を講ずるものとする。

第二章において国及び地方公共団体の個人情報の適正な取扱いを確保するために必要な施策を総合的に策定して実施する責務があるとされている。そして、政府の保有している個人情報の性質や目的等を勘案し、その個人情報の適正な取扱いが確保されるよう法制上の措置や必要な措置を講じなければならない。また、個人権利利益の保護を図るための適切な取扱いの確保も必要としている。更にそのためのさまざまな措置も講ずるものとしている。

国及び地方公共団体は個人情報保護の施策における責務を有するが、その方策としては組織内で統括する個人情報管理責任者を選定し、各部署においては個人情報保護対策の担当者を選任する。個人情報が管理体制の中でどのように流れているか、すなわち、個人情報の組織内での管理、利用、提供、廃棄がどのように行われているのかを把握した上で具体的な対策をとる。そして、個人情報保護に対する方針を定める。その方針としては、取得した個人情報の利用目的に関する方針、個人情報の管理において開示の求め等に対する方針、安全管理措置に対する方針等を決めておく。個人情報を直接、取扱う担当者に対する取扱いマニュアルの作成、又運営面での監査が求められる。実際に大事なのは、職員に対する個人情報保護に対する教育である。現実では、内部関係者による個人情報の漏洩事件が多々あるからである[11]。

4．情報セキュリティと個人情報の保護に関する施策

情報ネットワークの急速な発展は、私たちの生活に大きな変化をもたらした。そして、この情報ネットワークによって、世界中のコンピュータが接続されることにより、地理的、時間的超越のもとに随時に必要な情報を入手することが可能になった。それと同時に、今日のネットワーク社会に対して、多くの危険と障害が発生してきている。しかし、今後ともこの情報ネットワークの利便性を享受し、我々の生活の安全と社会の発展を進展させるためには情報のセキュリティが重要である。最近は情報セキュリティに対する関心が高くなり、情報管理に対する安全性が強く求められてきている。と同時に、個人情報の保護に関する関心も一層強くなってきた。

情報技術がめざましく進展することによって、国民の生活が便利になり、民間企業においては、電子商取引が進展し、また、国や地方公共団体においても電子政府や電子自治体による情報ネットワークシステムの構築がすすめられてきた。しかし、ネットワークに対する不正アクセスによるデータベースの破壊、データの改ざん、個人情報の漏洩などの個人情報保護に対する施策が必要である。個人情報がいったん漏洩し、それが、悪意を持った者の手に渡り、個人情報が不適正に取り扱われ、個人の権利利益が侵害される事件も起こると、深刻な被害をもたらし、社会問題にもなる。そのため、このようなネットワーク

社会の不正に対応する法的な対応策が強く求められるようになってきた。そのような社会的な要請のもとに、平成17年４月１日より、個人情報の保護に関する法律が施行されることになった。そこでさらに個人情報の保護に関する法律の第三章個人情報の保護に関する施策等について見てみることにしよう。

第三章　個人情報の保護に関する施策等[12)]

第一節　個人の保護に関する基本方針

第七条　政府、個人情報の保護に関する施策の総合的かつ一体的な推進を図るため、個人情報の保護に関する基本方針（以下「基本方針」という。）を定めなければならない。

２　基本方針は、次に掲げる事項について定めるものとする。

一　個人情報の保護に関する施策の推進に関する基本的な方向

二　国が講ずべき個人情報の保護のための措置に関する事項

三　地方公共団体が講ずべき個人情報の保護のための措置に関する基本的な事項

四　独立行政法人が講ずべき個人情報の保護のための措置に関する基本的な事項

五　地方独立行政法人が講ずべき個人情報の保護のための措置に関する基本的な事項

六　個人情報取扱事業者及び第四十条第一項に規定する認定個人情報保護団体が講ずべき個人情報の保護のための措置に関する基本的な事項

七　個人情報の取扱いに関する苦情の円滑な処理に関する事項

八　その他個人情報の保護に関する施策の推進に関する重要事項

３　内閣総理大臣は、国民生活審議会の意見を聴いて、基本方針の案を作成し、閣議の決定をもとめなければならない。

４　内閣総理大臣は、前項の規定による閣議の決定があったときは、遅滞なく基本方針を公表しなければならない。

５　前二項の規定は、基本方針の変更について準用する。

第二節　国の施策（第八条―第十条）

（地方公共団体等への支援）

第八条　国は、地方公共団体が策定し、又は実施する個人情報の保護に関する施策及び国民又は事業者等が個人情報の適正な取扱いの確保に関して行う活動を支援するため、情報の提供、事業者等が講ずべき措置の適切かつ有効な実施を図るための指針の策定その他の必要な措置を講ずるものとする。

（苦情処理のための措置）

第九条　国は、個人情報の取扱いに関し事業者と本人との間に生じた苦情の適切かつ迅速な処理を図るために必要な措置を講ずるものとする。

（個人情報の適正な取扱いを確保するための措置）

第十条　国は地方公共団体との適切な役割分担を通じ、次章に規定する個人情報取扱事業者による個人情報の適正な取扱いを確保するために必要な措置を講ずるものとする。

第三節　地方公共団体の施策

（地方公共団体等が保有する個人情報の保護）

第十一条　地方公共団体、その保有する個人情報の性質、当該個人情報を保有する目的等を勘案し、その保有する個人情報の適正な取扱いが確保されるよう必要な措置を講ずることに努めなければならない。

2　地方公共団体は、その設立に係る地方独立行政法人について、その性格及び業務内容に応じ、その保有する個人情報の適正な取扱いが確保されるよう必要な措置を講ずることに努めなければならない。

（区域内の事業者等への支援）

第十二条　地方公共団体は、個人情報の適正な取扱いを確保するため、その区域内の事業者及び住民に対する支援に必要な措置を講ずるよう努めなければならない。

（苦情の処理のあっせん等）

第十三条　地方公共団体は、個人情報の取扱いに関し事業者と本人との間に生じた苦情が適切かつ迅速に処理されるようにするため、苦情の処理のあっせんその他必要な措置を講ずるよう努めなければならない。

第四節　国及び地方公共団体の協力

第十四条　国及び地方公共団体は、個人情報の保護に関する施策を講ずるにつき、相協力するものとする。

第三章においては、個人情報の保護に関する施策について定めており、個人情報の保護に関する基本方針について、まず個人情報の保護に関する施策の基本的方向や国が講ずべき個人情報に対する措置について定めており、また地方公共団体、独立行政法人、個人情報取扱事業者等の講ずべき個人情報の保護のための措置、さらに、個人情報の取扱いに関する苦情の処理についても定めている。そして、国の施策として、地方公共団体が策定して実施する個人情報の保護に関する施策や個人情報の適正な取扱いの確保に関する活動を

支援するため必要な措置を講ずる。また、国は個人情報の取扱いにおける苦情処理に関しても、適切かつ迅速な処理を図るための措置も講ずるとしている。

そして、地方公共団体や地方独立行政法人においても個人情報の適正な取扱いが確保されるような措置を講ずるように努めなければならないとしている。また国と同様に個人情報の適正な取扱いを確保するために事業者や住民に対して支援に必要な措置を講ずるよう努めなければならないとしている。さらに、苦情に関しても地方公共団体は、個人情報の取扱いで生じた苦情が適正かつ、迅速に処理されるように苦情処理のあっせんや必要な措置を講ずるように努めることを求めている。

一般に情報は、ネットワークによって個々のコンピュータが通信回線で接続されることによって、その価値は一段と高まる。そして、集積された個々の情報は連携することによってその価値を更に高めていく。それは個人の情報においても同様なことであって、それが情報ネットワークによって瞬時に遠隔地間でも利用可能である。このことは過疎化の進んだ遠隔地での利用にも有用であることから、遠隔医療や福祉の面においても利用が期待できる。しかし、もし医療や福祉関係で蓄積された個人情報が、当事者の意思とは無関係に売買され利用され、悪用された場合、個人の名誉や人権の侵害になることもある。このようなことから、個人情報の保有者や管理者および利用者に対して法的な保護制度が求められる[13]。

最近では、情報ネットワークが普及するとともに、商取引などで蓄積されたデータベースにおける個人情報の管理の問題が、個人情報の保護に関して深刻な問題を提起してきている。商取引で集められた顧客の信用情報や顧客の資産情報および取引内容などがデータベース化された情報は、それ自身で高価な商品価値を持っており、それは営業活動に利用可能であることから、商品として売買の対象となりかねないからである[14]。

現在では、行政においても個人情報の保護に関する環境整備は重大な課題である。行政機関は個人情報保護のためには、個人情報のファイルの保有に関しては掌握事務の遂行に必要な場合に限り、その目的に必要な範囲で業務を遂行し、個人情報の漏洩などがないように安全確保の措置をとる必要がある。また、国民においては自己の情報の開示請求権が認められている[15]。

個人情報は、単体ではその情報に対する価値は低い、例えば、名前のみだけの情報だけでは、情報としての利用価値は低い。しかし、その名前の情報に住所や電話番号をはじめとする多くの情報が結合された場合にその情報に対する価値が高くなる。そのため、個人情報の保管管理に際し、分離して個別の情報を保管しておくことも、一方策である。

また、個人情報の漏洩は正規の職員によって引き起こされる場合がある。そのため、組織内の個人情報保護に対する教育と漏洩防止の体制づくりが求められる。個人情報の漏洩は、組織が間接的に社会的信用を失うだけでなく、場合によっては損害賠償も伴う[16]。

このようなことから、組織的安全管理が必要である。個人情報に対する組織的安全管理

においては管理に対して従業員の責任と権限を明確にし、手順書を作成し、管理の実施状況を確認する。組織的安全管理においては、個人情報保護に関する方針、組織体制の整備、個人情報取扱い手順書の整備、組織的安全管理の評価、見直しや改善と漏洩事件に対する対処等に取り組んでおく。まず、組織内における個人情報の管理について役割を分担し、責任も明確にしておき、安全管理のための組織体制を整えなければならない。また、個人情報を扱う情報システムについて運用の責任者も設置する必要がある。さらに、個人情報保護の実現のために規程を置いて、そのためのマニュアルも整えておかねばならない。

個人情報管理者を設置し、規程を定めるとともに組織体制を整えて、技術的な措置を施すとともに、従事者に対する教育および研修が必要である。教育および研修は従事者と正規の職員だけでなく嘱託職員、契約職員、派遣職員を含む職員に対しても必要である。個人情報の漏洩事件が委託先の従事者による流出や取扱いのミスによって起こっていることもあるので人的な管理体制も重要である。また、技術的な安全管理体制も必要である。技術的安全体制とは、個人情報の漏洩や消滅および棄損の防止のために個人情報を取扱う情報システムに対し、個人情報への不正アクセスの制御、個人情報の暗号化、個人情報を取扱う情報システムに対する管理体制である[17]。

5．個人情報の保護に関する法律の施行と実状

特に行政機関は個人情報保護のためには、人格尊重の下で慎重な取扱いが求められる。個人情報の取扱いに関しては、その目的に必要な範囲で業務を遂行し、個人情報の漏洩などがないように安全確保の措置をとる必要がある[18]。

この個人情報保護に関する法律は、特定の個人を識別可能な情報については全て保護しようというものである。そのため、行政機関において、個人情報の取扱いに対する基本原則を設けて、個人情報が個人の人格尊重の下で、慎重に取り扱われるべきであるとして、それの下に業務を遂行することとしている。すなわち個人情報の利用目的による制限、適正な取得、正確性の確保、安全性の確保、透明性の確保に則して機関、法人、団体および個人において個人情報保護のために、適正な取扱いをすべきであることを規定し業務を遂行している[19]。

個人情報の保護に関する法律は平成15年12月10日の公布の施行政令によって、平成17年４月１日に施行された。この個人情報の保護に関する法律は、紆余曲折を経てやっと施行されたものである。その結果、本法が施行されるまでは、民間事業者に対して、今までそれほど法規制がなかったこともあり、個人情報の取扱いに対する意識は低かったと言えるが、この個人情報の保護に関する法律が施行されて以後、公的機関においても、民間事業者においても個人情報の取扱いに対する意識は高まってきたと言える[20]。

そして、行政において今日の情報化社会で、情報に関して法によって、いかに規律していくかという施策である。しかし、今後、公的な機関によって、個人的な情報、すなわち、氏名、住所、電話番号を初め、納税額、職歴、経済状態などが特定の権力によって集中管理されることとなる[21]。

しかし、国及び地方公共団体は個人情報保護の対しては、個人情報の適正な取扱いを確保するために必要な施策を総合的に策定して実施する責務がある。そして、個人情報の適正な取扱いが確保されるよう法制上の措置や必要な措置を講じなければならない。また、個人の権利および利益の保護を図るための適切な取扱いの確保も必要としている。国の施策として、地方公共団体が策定して実施する個人情報の保護に関する施策や個人情報の適正な取扱いの確保に関する活動を支援するため必要な措置を講じなければならない。さらに、苦情に関しても地方公共団体は、個人情報の取扱いで生じた苦情が適正かつ、迅速に処理されるように苦情処理のあっせんや必要な措置を講ずることが求められる。

このように個人情報保護に対する法律が施行されたが、さらにこれらを強化するためにはセキュリティポリシーに基づいた情報セキュリティ対策が必要である。

6．セキュリティポリシーと情報セキュリティ対策

情報セキュリティの目的は機密性、完全性、可用性である。機密性はアクセス権を持つ者だけがデータや情報を入手することであり、完全性は情報や情報システムが完全に保護されることである。そして、可用性はアクセス権を持つ利用者が随時に必要な情報にアクセスできることを確実にすることである。そして、そのためにはセキュリティポリシーの策定を実施し、組織内での情報セキュリティに対する体制を整えなければならない。

セキュリティポリシーとは組織が保有している情報資産に対し、ネットワークを介してのリスクに対して、予防、検知および回復について計画的、組織的に取り組む方針である。要するに、セキュリティポリシーはセキュリティに対する組織方針あり、セキュリティポリシーの策定は組織の経営陣の協力と支援の下に取り組み、実施されねばならない。そして、セキュリティポリシーの策定は組織が保護しなければならない重要な情報資産を特定し、担当者が義務と責任を明確にして実施しなければならない。

セキュリティポリシーの策定は、セキュリティに対する意識と認識のもとに、まずセキュリティに対する目標と適用範囲を明確にし、次にセキュリティの対象とする情報システムやネットワークシステムを明確にし、そのシステムで取扱い運用している情報資産も特定し明確にする。次に、対象となったシステムや情報資産のリスクを分析し、これを明確にする。そして、この明確化したセキュリティ対象のリスクの分析結果をセキュリティポリシー策定に効果的に活用していく[22]。

かつて、情報セキュリティは各種情報や情報システムおよびネットワークの安全性を確保することが求められてきた。しかしさらに、情報セキュリティの要素としては守秘性、安全性、可用性があげられる。守秘性は個人のプライバシーや情報の秘密を遵守することである。安全性は情報の改ざんや破壊を防止することである。そして、可用性は必要な時に必要な情報を適切に入手でき利用できることである。今日のネットワークにおける不正行為から情報セキュリティを確保するためには、次のような対処方法があげられる。一般的に情報セキュリティの対処方法としては、抑止、防止、検出、回復といった段階で実施する。抑止はネットワーク等に対する不正行為を法的な処罰等によって対応することを事前に周知させることによって抑制することである。不正行為に対する意欲を事前に削ぐ事といえる。防止は情報の暗号化やセキュリティソフト等によって情報の漏えいを未然に防ぐことである。検出は不正行為が実際に発生した場合に、ログ等からその実態を把握することである。速やかな検出により適切な対処は被害の拡大を防ぐことにつながる。回復は不正行為による被害の状況を適切に把握し、正常な状態に復帰させることである。そのためには、バックアップをとっておき、回復のための体制を整えておくことが大切である。

一般に情報セキュリティの対策には多くの費用がかかる。また、システムも使い勝手が悪くなる場合もある。しかし、セキュリティ対策を怠ると、致命的な損害を被ることもあり得る。これらを回復させるためには、被害の状況によっては、情報セキュリティ対策に費やした以上の費用が必要な場合がある。さらにそれだけではなく、信用の失墜にも繋がる。場合によっては回復が困難である場合もあり得る。そのため、情報システムの導入当初から情報セキュリティ対策を検討し、情報を特性に応じた情報セキュリティ対策を施さなければならない。

セキュリティ対策として、まず、セキュリティのための組織を構築し、それぞれの役割と責任を明確にしておく。さらに、情報セキュリティを実施するためにはセキュリティポリシーとして、その目的、対象とする範囲、責任体制、守るべき対象、セキュリティ対策の基本などを明確にして、明文化も必要である。そして、情報セキュリティ対策を実施するにあたっては、その組織の構成員および関係者に情報セキュリティに対する対策について周知させておくとともに、各自の責任を認識させ、情報セキュリティに対する重要性を十分に理解させておかねばならない[23)]。

セキュリティ機能としては、セキュリティの予防機能、検知機能や回復機能などが挙げられる。予防としてはネット犯罪の拡大を防止し、検知機能により不正や障害を速やかに発見し通知する。そして、もし、ネットワークの障害に陥った場合には障害から回復機能によって障害から速やかに正常な状態に回復させねばならない。

7．おわりに

情報ネットワークが単なるファイル転送であった時代から、インターネットに発展し、それが各個人のコミュニケーションの手段として利用されてきたが、現在では更に発展し、現代社会や生活文化に、更に行政および政治にも大きな変革をもたらそうとしている。しかし、このような情報ネットワークの急速な進展に対し、最近では特にインターネットをめぐって、多くの法的問題が噴出してきている。インターネット上での表現内容に関するもので、誹謗中傷や名誉毀損などの問題やインターネットを利用した詐欺的行為などの問題である。

ネットワーク社会の進展に伴って、最近では不法侵入や個人情報に対する諸問題が社会的に問題視され、社会的規制が求められるようになってきた。これらの問題に対し、倫理的規制と法的規制での対処が考えられる。情報技術が益々進歩するのにともなって、ネットワークの不正も高度化し巧妙化してきている。これらに対し、社会的規制が強く求められるようになるとともに、個人情報の保護の問題が重要視されるようになってきた。

最近、個人情報の保護に関する法律が完全施行されて以降、個人情報に対する意識が過剰になったようである。今まで発行していた会員名簿の発行をやめたり、問い合わせなどにも、個人情報の保護を理由に拒否する事態もみられるようになってきた。個人情報に対する意識過剰は、社会活動や経済活動にも影響をもたらしかねないかもしれない。そして、個人情報に対する意識過剰と個人情報保護に対する対策と調整をいかに行うかが今後の施策に求められる。この個人情報の保護を強化するためには、セキュリティポリシーの策定と情報セキュリティの体制が必要である。

セキュリティポリシーの策定については、組織内の各部門の情報セキュリティ担当者を明確にし、更に、各部門から状況に応じて、必要な意見を聴取して、セキュリティポリシーの策定の段階から組織内で情報セキュリティに対する認識と理解を深めておかねばならない。さらに、セキュリティポリシーは組織の幹部および情報システムの管理者やセキュリティ対策関係者で構成し、セキュリティポリシーの目的、権限や業務などを策定し、責任の所在についても明確にしておくことが必要である。そして、情報セキュリティの対策としては、技術的対策と運用管理対策とが考えられる。技術的対策としては、当然、セキュリティ・ツールを導入するとともに、運用管理対策として、情報セキュリティポリシーの策定と人材育成を図ることが望まれる。

引用・参考文献

1）渡辺和彦・坂田哲也・飯田秀樹・斎藤南哲、ネットワークシステム、2000、16-18。
2）大保久哉・羽田晋朗・高野一彦、個人情報保護法対策、九天社、2005、２-21。
3）園部逸夫編、個人情報保護法の解説、ぎょうせい、2005、７-８。
4）東京海上日動リスクコンサルティング、個人情報保護とリスクマネジメント、ソフトリサーチセンター、2004、15-19。
5）菅原俊一・小中居学・中山章子、個人情報保護法とプライバシーマーク取得の実務、日本法令、2005、13-16。
6）園部逸夫編、 個人情報保護法の解説、ぎょうせい、2005、９-36。
7）藤原宏高、個人情報保護法、株式会社カットシステム、2004、427-429。
8）園部逸夫編、個人情報保護法の解説、ぎょうせい、2005、40-41。
9）園部逸夫編、前掲書、2005、45-68。
10）日本ネットワークセキュリティ協会編、個人情報保護法対策、インプレス、2003、198-199。
11）大保久哉・羽田晋朗・高野一彦、個人情報保護法対策、九天社、2005、30-41。
12）重本優治、プライバシーマーク、翔泳社、2005、３-４。
13）石村善治・堀部政男編、情報法入門、法律文化社、1999、76-78。
14）夏井高人、ネットワーク社会の文化と法、日本評論社、1997、184。
15）和田英夫・原田三郎・日笠完治・鳥居壮行、情報の法と倫理、北樹出版、1999、118-120。
16）岸田　明監修、事例で学ぶ個人情報保護、富士通オフィス機器株式会社、2005、９-12。
17）渡部喬一、個人情報保護法のしくみと実務対策、日本実業出版社、2005、114-132。
18）和田英夫・原田三郎・日笠完治・鳥居壮行、情報の法と倫理、北樹出版、1999、118-120。
19）岡村久道・新保史生、電子ネットワークと個人情報保護、経済産業調査会、2002、511-513。
20）北岡弘章、個人情報保護と対策、日経BP社、2005、11-12。
21）堀部政男監修、鈴木正朝、個人情報保護法とコンプライアンス・プログラム、商事法務、2004、１-２。
22）森　真一、塩谷幸治、新川晃太郎、セキュリティポリシーの考え方、株式会社エスシーシー、2001、18-69。
23）宮地充子、菊池浩明編著、情報セキュリティ、オーム社、2003、１-16。